2006

A Methodology for the Examination of the Effectiveness of Secure Erasure Tools Running On Windows XP - Research in Progress

Anthony Hadfield
Edith Cowan University

Michael Ahern
Edith Cowan University

Leo Sell
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

A Methodology for the Examination of the Effectiveness of Secure Erasure Tools Running On Windows XP – Research in Progress

Anthony Hadfield
Michael Ahern
Leo Sell
Andrew Woodward
School of Computer and Information Science
Edith Cowan University
ahadfiel@student.ecu.edu.au
mahern@student.ecu.edu.au
lsell@student.ecu.edu.au
a.woodward@ecu.edu.au

Abstract

Currently, there appears to be a lack of academic research in the area of testing the efficacy of secure erasure applications and utilities in regard to the activities of an average user in a home or small business context. This research in progress aims to develop a testing methodology that will provide a forensically sound base for which to analyse these tools. It involves the installation of various Internet related applications (for example browsers, instant messaging software and download clients), and the use of these applications for typical Internet activities (e.g. internet banking, instant messaging, web browsing and other activities that would be conducted by an average user). Following the creation of the simulated history, this paper discusses a practical testing methodology that includes the creation of image files, the allocation of these image files, and the use of forensic tools to examine disk contents before and after the execution of the secure erasure applications on the simulated user history. Additionally, a reporting mechanism has been formulated that will allow test results to be efficiently compiled and compared to form valid conclusions about the effectiveness of each erasure utility on internet history.

Keywords
Erasure software, internet activity, digital forensics

INTRODUCTION

There are many commercial secure erasure tools available that are targeted towards different user types and operating systems (C/Net, 2006). There is also limited research into the efficacy of these tools for erasure of internet and other computer related activity. For example, Jones and Meyler (2004) examined the effect of selected erasure tools using the Windows NT and Windows 98 operating systems (OS). The authors concluded that there was sufficient information left to enable a forensic investigator to determine a trail of activity. These operating systems are no longer supported by Microsoft, and forensic practitioners now rarely come across computers which use these as their OS's. Preliminary analysis suggests that there is little research that has been conducted for the purpose of testing the security and efficacy of secure erasure applications on the Windows XP Service Pack 2 operating system.

This paper details a testing and experimentation methodology suitable for this purpose. The final methodology is designed with forensic validity, integrity and test reproducibility as primary objectives, and will result in a robust mechanism for testing these utilities under Windows XP SP2. Additionally, an objective is to produce a testing methodology that can be applied for testing similar tools on alternative operating systems, or for users with different needs (e.g. business, government, education and other groups with an interest in preserving confidentiality of records).

Various secure erasure utilities have been evaluated and selected based on consumer popularity and features offered (Tucows, 2006).

TEST PLATFORM DESIGN

The experimental tests used to determine the effectiveness of the secure erasure utilities are ideally to be conducted on a set of computers with identical configurations with regard to hardware, software and storage. The use of identically specified test machines will ensure that experiments and subsequent findings will be consistent, verifiable and reproducible.

TEST SOFTWARE OVERVIEW

A variety of commercial secure erasure applications and utilities have been selected on the basis of reported popularity, and similarity of claimed features (Tucows, 2006). These applications will be installed on separately imaged partitions for testing. These software products vary in price and origin; however they portray a reasonable and accurate representation of typical erasure tools available to consumers and organisations. Application version and vendor information are recorded in Table 1.

Table 1.0 Details and Versions of Secure Erasure Applications

Application Name	Version/Build #	Vendor
Anti Tracks	6.9.2	RIGHT Utilities Incorporated
Cyber Scrub Privacy Suite	4.0	Cyber Scrub LLC
R-Wipe & Clean	6.5 / 1238	R-tools Technology Incorporated
Tracks Eraser Pro	5.7	AceSoft
Window Washer	6.0	Webroot Software Incorporated

Anti Tracks

Anti Tracks is a secure erasure utility produced by RIGHT Utilities Inc.. It is designed to erase a variety of Internet activity history elements (refer Table X.X), and perform similar functionality on Microsoft Windows. For added flexibility, the program is upgradeable and updateable with modules that extend the application's operations to new software, or software that is not initially included in the release (RIGHT Utilities, 2006).

Cyber Scrub Privacy Suite

Cyber Scrub Privacy suite is a secure erasure package produced by Cyber Scrub LLC. Cyber Scrub performs typical secure erasure functions, and its main release is operational on a range of Internet and Windows applications. Additionally, Cyber Scrub also includes support for removable media, such as USB memory modules and storage media (CyberScrub LLC, 2006).

R-Wipe & Clean

R-Wipe & Clean was designed and produced by R-Tools Technology Inc.. Including functional capabilities typical of most secure erasure utilities, R-Wipe & Clean offers some unique features and functions. For example, R-Wipe offers users the facility to create customisable wipe lists. This allows for a more individualised erasure profile, and allows some information that the user may wish to retain to be kept, whereas other utilities may not differentiate (R-Tools Technology Inc., 2006).

Tracks Eraser Pro

Tracks Eraser Pro is a software utility produced by AceSoft. Like Anti Tracks, Tracks Eraser Pro is updateable and upgradeable with additional downloadable modules that extend Tracks Eraser Pro's functionality to include programs and applications that were not addressed at the time of initial release. This also allows the user to reduce the time needed for secure erasure operations to complete as they can eliminate not-installed programs from Tracks Eraser's wipe list (AceSoft, 2006).

Window Washer

Window Washer is a secure erasure utility produced by Webroot Software Inc. Window Washer includes functionality that is typical for most secure erasure applications, including web browser history deletion and secure erasure options. Window Washer also includes some Microsoft Windows extensions that allow the program to integrate with the operating system and provide functions such as Bleach and Shred (Webroot Software Inc., 2006).

WRITING HISTORY

To simulate an average user's typical Internet application usage, a variety of programs were installed and used. These include Web browsers, media applications and peer-to-peer, download and instant messaging clients. For full details of the installed software, please refer to Table 2.0.

Table 2.0 Comparison of Erasure Software Claims

	Anti Tracks	Privacy SuiteCyber Scrub	& CleanR-Wipe	Eraser ProTracks	WasherWindow
Address bar history (Firefox)	✓	✓	✓	✘	✓
Address bar history (IE)	✓	✓	✓	✓	✓
Address bar history (Mozilla)	✓	✓	✓	✘	✓
Address bar history (Netscape)	✓	✓	✓	✓	✓
Address bar history (Opera)	✓	✓	✓	✓	✘
Cookies (Firefox)	✓	✓	✓	✘	✓
Cookies (IE)	✓	✓	✓	✓	✓
Cookies (Mozilla)	✓	✓	✓	✘	✓
Cookies (Netscape)	✓	✓	✓	✓	✓
Cookies (Opera)	✓	✓	✓	✓	✘
Temporary Internet files	✓	✓	✓	✓	✓

Internet history files	✓	✓	✓	✓	✓
History of auto complete	✓	✓	✓	✓	✘
Index.dat	✓	✓	✓	✓	✘
Windows temp files	✓	✓	✓	✓	✘
Registry	✓	Ⓟ	✓	Ⓟ	Ⓟ
P2P	Ⓟ	✓	✘	✓	✘
Instant Messaging	Ⓟ	✓	✓	✓	✘
'Secure Erase' facility	✓	✓	✓	✓	✘
'Schedule' facility	✓	✓	✓	✓	✓
'Profile' selection	✓	✓	✘	✘	✘
Ⓟ = Additional plug-in / configuration required.					

Table 3.0 Details and Versions of Installed Software Applications

Application Purpose	**Application Name**	**Version / Build #**	**Vendor**
Internet Browsers	Internet Explorer	6.0	Microsoft Corporation
	Firefox	1.5.0.4	Mozilla
	Mozilla	1.8b	Mozilla
	Netscape	7.2	Netscape Communications Corporation
	Opera	9.01 / 8552	Opera Software ASA
P2P / Download Clients	Limewire	4.1.26	Limewire LLC
	BearShare	6.0.0.23778	Music Lab LLC
	BitTorrent	4.24.0	Open Source
Instant Messaging	MSN Messenger	7.5 / 7.5.0324	Microsoft Corporation
Media Programs	iTunes	7.0.1.8	Apple Computer Incorporated
	Quicktime	7.1.3	Apple Computer Incorporated

Once installed, the programs will be used in a manner that will simulate the experience and practices of an average computer user. These activities shall include:

- Internet banking – typical Internet banking activities are to be conducted using each of the Internet browsers installed.

- Web browsing – installed Web browser software will be used to access a variety of websites with different content, browser requirements, and authorship demographics.
- Streaming media – various applications are to be used to stream real-time music and video media over the Internet.
- Peer-to-peer activity – various files will be downloaded from peer-to-peer network clients to simulate the average user downloading music, software, images or documents.
- Instant messaging – the instant messaging client will be configured with a simulation account and used to communicate with another instant messaging user.

BROWSER HISTORY MANAGEMENT

Browser history is stored and managed differently by each browser (Belani & Jones, 2005). Whereas some browsers make use of index files to cache Internet files, others use temporary and/or hidden directories for the storage of transient information.

Microsoft Internet Explorer

Internet Explorer stores browser history under an individual user(s)' Windows profile. Windows operating systems (from Windows 2000 onwards) maintain an individual profile for each user, including their own "My Documents", "My Pictures" and "My Music" folders, which are hidden from other non-administrator users. Included is the location "Temporary Internet Files", where Internet Explorer maintains the primary cache(s). A typical file path for this folder could be:

C:/Documents and Settings/[Username]/Temporary Internet Files

Cookies are typically stored in a similar fashion:

C:/Documents and Settings/[Username]/Cookies

History without content is stored in a file named "index.dat." (Belani & Jones, 2005).

Mozilla, Mozilla Derivatives (Firefox), and Netscape

These browsers (and other web browsers based on them) store history information in a similar fashion to Internet Explorer (IE). Like IE, these browsers store Internet history in a single file without cached content, called 'history.dat'. A significant difference between Internet browsers of this class, and Internet Explorer, is the technique used to store the cached information. Whereas the index.dat file is constructed in binary format, the history.dat file is stored as ASCII. This makes it marginally easy to forensically analyse and extract. A typical storage location for a Firefox Internet history is:

C:/Documents and Settings/[Username]/Application Data/Mozilla/Firefox/Profiles/history.dat. (Belani & Jones, 2005).

DISK IMAGING PROCEDURES

Prior to any testing or imaging activities, all hard drives and storage devices to be used for experimental purposes should be securely erased using a forensically sound erasing procedure. This will reduce the possibility of erroneous or misleading results when further testing and analysis are performed.

Initially, Microsoft Windows XP Service Pack 2 will be installed on the test machine on drive C (primary hard disk). This will allow the installation of partition management software, and remaining

hard drives and space to be organized into separate partitions suitable for installation and execution of secure erasure tools.

Drive partitioning will be accomplished by using partition management software (e.g. Partition Manager, Partition Magic) to divide primary and secondary hard disks into a series of smaller partitions. There are several reasons for this: secure erasure and image management operations are significantly less time intensive on smaller disk sizes when compared to using the space available on an entire hard disk, and it allows the test machine to host redundant Windows images, which are to be subsequently customized to make them viable for testing purposes.

Additionally, the use of a HELIX Live 1.7 Linux CD and Autopsy 2.06 (sourced prior to version 1.8 release) as a forensic tool will require a partition to be created as an EXT3 system for the forensic creation of images and extraction of recoverable files.

Programs to be installed to simulate the typical configuration of an average user include various web browsers (Opera, Microsoft Internet Explorer, Netscape, Mozilla Firefox), peer-to-peer (P2P) and download applications (Limewire, Bearshare, BitTorrent) and instant messaging clients (MSN Messenger), and media applications (Quicktime, iTunes). Some of the erasure tools are able to be customised in terms of what they erase, but this requires a reasonably high level of technical knowledge. An assumption is made that someone with such in-depth technical knowledge would not be relying on such erasure software to remove evidence of their activity, so these applications will be installed in their default mode. They will then be used, and a typical usage history simulated. Activities to be conducted included Internet banking, video-streaming, file downloads, music streaming, email access, Internet browsing and other typical uses of Internet applications.

This test installation of Windows XP SP2 (with Internet activity and usage history included) will then be imaged using the "dd" utility in Helix to become a base platform from which to install and test the various secure erasure programs. Subsequently, the test images are to be loaded, and a secure erasure application installed. The resulting installation will then be re-imaged via the same procedure, and the process repeated for each of the secure erasure programs. These images are then to be placed in separate partitions on the test machine.

A base installation of Windows XP SP2 will be created and installed on the first partition of the primary hard drive on the test machine. Additionally, "dd" will again be utilised to create a backup image (to be installed on the secondary drive). This will allow for a clean install of Windows XP SP2 to be duplicated or reinstalled in the event of mistake, error, or equipment failure. In the operational partition, the installed version of Windows XP Service Pack 2 will be modified to include typical Internet applications for a variety of purposes.

VERIFICATION OF IMAGE INTEGRITY

Subsequent to installation, the images shall be verified using MD5 and SHA1 hash algorithms. SHA1 was selected as it is the current United States Government standard for cryptographic hash algorithms (National Institute of Standards and Technology, 2002). Hashing provides an accurate representation of the data through a mathematical algorithm, and can be used forensically to verify the integrity and validity of images through comparison and re-calculation (Department of Justice/Office of Justice Programs, 2004). Under Helix, hash calculations can be performed using the "md5sum" and "sha1sum" commands.

Images will be hashed at a number of points to verify their integrity, and to validate the transfer methods employed (refer to Image Transfer section) as being able to provide bitwise transfers. Hash calculations shall be made at various key stages:

- Post-image file installation – following the formation of the individual image files with their respective installs of the simulated user history and the secure erasure utility in question.

- Post-execution – Following the execution of the secure erasure utility and its subsequent formation of a new image file.
- Post-sever transfer – Subsequent to the transfer of the image files to the ECUIS lab storage server.
- Post-analysis machine transfer – Following the transfer of the image files from the server to the analysis machines.

FORENSIC ANALYSIS

There are a variety of forensic tools available which can be used evaluate the results of secure erasure utility execution, both proprietary and open source. The primary forensic tool to be employed is Autopsy, an open-source component of the Helix information security and electronic investigation suite (Spenneberg, 2003). Autopsy is a browser-based application that enables images to be analysed, and for specific file types and fragments to be searched for, identified and extracted for further evaluation (Altheide 2004).

Utilities designed for the gathering of Internet history are also to be employed. These include Web Historian, a freeware utility that is compatible with a variety of Internet browsers including Internet Explorer, Opera, Netscape and Mozilla derivatives (Mandiant, 2006). Web Historian functions by analysing caches and indexes, and exports the analysis results into a Microsoft Excel spreadsheet of identified Internet activity evidence. Preliminary testing using Anti Tracks and Tracks Eraser Pro validates Web Historian as a forensically sound tool for examination of Internet history – results of the pre- and post-erasure analysis by Web Historian showed that the erasure utilities performed as expected, and as directed. Consequently, Web Historian will be used in all further testing activities.

As a control, post-erasure images will also be examined with Windows Explorer to attempt to ascertain what information is recoverable, and what information (if any) appears to be erased. Analysis using Windows Explorer also enables the project to better simulate the experience of a user unversed in digital forensics practices by displaying what they are likely to see when they assume that a file, folder or combination thereof has been removed.

REPORTING PROCEDURE

A standardised reporting form will be created and utilised in each instance of testing. For each test, key details are to be recorded including time and date of test, version and installation information of the secure erasure utility being tested. The reporting mechanism will also include any differences in hardware or software configurations on the test platforms.

The development of a standing reporting form enables test results to be compiled and recorded under a uniform structure, and allows tests to be repeated under the same conditions for verification, or repetition of the intended experiments.

CONCLUSION

This research in progress outlines a methodology for testing the efficacy of commercially available secure erasure utilities in regards to the context of an average home/small business user. Specifically, a method for the simulation of such a history has been discussed, including appropriate applications and activities. Additionally, a testing procedure has been discussed that should allow for valid, reproducible research and testing to be conducted in this area, with a suitable recording and reporting mechanism as a component.

Academic research in this field is necessary to produce meaningful and relevant results that can be used by both users and practitioners. End users can determine whether a particular application will suit their requirements, and electronic evidence practitioners can use the information for forensic purposes.

REFERENCES

Acesoft. (2006). Delete *History – Features of Tracks Eraser Pro*. Retrieved 13/10/06 from: http://www.acesoft.net/features.htm

Altheide, C. (2004). Forensic analysis of Windows hosts using UNIX-based tools. *Digital Evidence* **1:(3)** pp 197-212

Belani, R., & Jones, K. (2005). *Web Browser Forensics, Part 1*. Retrieved 18/10/06 from: http://www.securityfocus.com/infocus/1827

C/Net Download.com. (2006). *Online Privacy – Erasure Utilities.* Retrieved 20/10/06 from: http://www.download.com/Online-Privacy/3150-2144_4-0.html?tag=dir

CyberScrub LLC. (2006). *Erase Delete Wipe Overwrite Data With CyberScrub.* Retrieved 15/10/06 from: http://www.cyberscrub.com/products/privacysuite/index.php

Jones, A. & Meyler, C. (2004). What evidence is left after disk cleaners? *Digital Evidence* **1:(3)** pp 183-188

Mandiant. (2006). *Intelligent Information Security – Web Historian.* Retrieved 19/10/06 from: http://www.mandiant.com/webhistorian.htm

National Institute of Standards and Technology. (2002). *Federal Information Processing Standards Publication 180-2: Secure Hash Standard.* Retrieved 22/10/06 from: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

RIGHT Utilities Inc. (2006). *Anti Tracks – Protect Your Privacy and Improve System Performance*. Retrieved 16/10/06 from: http://www.rightutilities.com/products/antitracks/anti-tracks.htm

R-Tools Technology Inc. (2006). *Disk Wipe and Clean Software to Delete and Erase Data, Files or Clean Disk Space*. Retrieved 15/10/06 from: http://www.r-wipe.com

Spenneberg, R. (2003). *Autopsy and Sleuthkit, the Digital Forensics Toolkit: The Tracker Dog's Guide.* Retrieved 18/10/06 from: http://www.linux-magazine.com

Tucows. (2006). *File Management: Disk Cleaner Downloads.* Retrieved 21/10/06 from: http://www.tucows.com/Windows/IS-T/FileManagement/DiskCleaners/

United States Department of Justice (Office of Justice Programs). (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Retrieved 15/10/06 from: http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Webroot Software Inc. (2006). *Window Washer: Features*. Retrieved 18/10/06 from: http://www.webroot.com/consumer/products/windowwasher/features.html

COPYRIGHT